CLAIMS

What is claimed is:

1. A method of detecting an attack on an authentication service, said method comprising:

storing data relating to a plurality of requests communicated to an authentication service from a plurality of user agents via a data communication network,

searching the stored data based on a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user agents, and

comparing the stored data associated with each of the identified requests with a predefined pattern characterizing an attack to determine when the identified request indicates the characterized attack on the authentication service.

2. The method of claim 1, wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following:
a network address from which one of the plurality of the requests is communicated; a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests; a status of the one of the plurality of the requests; a time stamp indicating a date and time of the one of the plurality of the requests; a type of interface from which the one of the plurality of the requests is

communicated; and the user agent from which the one of the plurality of the requests is communicated.

3. The method of claim 2, wherein said status of the one of the plurality of the requests comprises one of more of the following: the one of the plurality of the requests is successful; the one of the plurality of the requests is unsuccessful; and the user account associated with the one of the plurality of the requests has been locked.

4. The method of claim 3, wherein said storing the data relating to the plurality of the requests comprises storing a password associated with the one of the plurality of the requests if the one of the plurality of the requests is unsuccessful.

5. The method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using a single password to unsuccessfully attempt at least a predetermined quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the multiple user accounts within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the single network address within the predefined time interval.

6. The method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple passwords to unsuccessfully attempt at least a predetermined quantity of requests on a single user account within a predefined time interval; using the multiple passwords to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the single user account within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests on the single user account within the predefined time interval.

7. The method of claim 1, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: a single password to unsuccessfully attempt at least a predetermined quantity of requests from multiple network addresses on a single user account within a predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the multiple network addresses on the single user account.

8. The method of claim 1, further comprising generating a report if it is determined that one or more of the identified requests indicate the characterized attack, said report providing information regarding the attack for use in defending against the attack.

9. The method of claim 1, further comprising remedying the attack if it is determined that one or more of the identified requests indicate the characterized attack.

10. The method of claim 9, wherein said remedying the attack comprises performing one or more of the following: locking a user account associated with one of the plurality of the requests; blocking a network address from which the one of the plurality of the requests is communicated; implementing a human interaction proof on the authentication service; prompting a user to change a password associated with the user account; and limiting a quantity of allowed unsuccessful requests to a predetermined quantity within a predefined time interval for the network address from which the one of the plurality of the requests is communicated.

11. The method of claim 1, wherein the plurality of the requests comprises one or more of the following types of requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated.

12. The method of claim 11, wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to unsuccessfully attempt at least the predetermined quantity of the requests on multiple human interaction proof strings within the predefined time interval.

13. The method of claim 1, wherein said comparing the stored data associated with each of the identified requests with a predefined pattern comprises:

comparing historical data relating to the authentication service with the stored data, and

in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred.

14. The method of claim 1, wherein said searching the stored data to identify at least one of the plurality of the requests comprises searching the stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts, and a time interval during which one or more requests are communicated;

wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables.

15. The method of claim 1, wherein one or more computer-readable media have computer-executable instructions for performing the method recited in claim 1.

16. A system of detecting an attack on an authentication service, said system comprising:

a first memory area to store data relating to a plurality of requests communicated to an authentication service from a plurality of user agents via a data communication network, said data being stored in the first memory area as a log of the authentication service;

a second memory area to store a predefined pattern of one or more requests, said predefined pattern characterizing an attack on the authentication service; and

a processor configured to execute computer-executable instructions to:

search the stored data as a function of a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user agents,

compare the stored data associated with each of the identified requests with the predefined pattern, and

determine whether the identified request indicates the attack characterized by the predefined pattern.

17. The system of claim 16, wherein the stored data comprises one or more of the following: a network address from which one of the plurality of the requests is communicated; a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests; a failed password associated with the one of the plurality of the requests; a status of the one of the plurality of the requests; a time stamp indicating a date and time of the one of the plurality of the requests; a type of interface from which the one of the plurality of the requests is communicated; and the user agent from which the one of the plurality of the requests is communicated.

18. The system of claim 16, wherein said predefined pattern is characterized by one or more of the following: using a single password to unsuccessfully attempt a quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt the quantity of the requests from a single network address on the multiple user accounts within the predefined time interval; and unsuccessfully attempting the quantity of the requests from the single network address within the predefined time interval.

19. The system of claim 16, wherein said predefined pattern is characterized by one or more of the following: using multiple passwords to unsuccessfully attempt a quantity of requests on a single user account within a predefined time interval; using the multiple passwords to unsuccessfully attempt the quantity of the requests from a single network address on the single user account within the predefined time interval;

unsuccessfully attempting the quantity of the requests on the single user account within the predefined time interval; using a single password to unsuccessfully attempt a quantity of requests from multiple network addresses on a single user account within a predefined time interval; and using the multiple network addresses to unsuccessfully attempt the quantity of the requests on the single user account.

20. The system of claim 16, wherein the processor is configured to search the stored data to identify at least one of the plurality of the requests by generating a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts, and a time interval during which one or more requests are communicated; wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables.

21. The system of claim 16, wherein the processor is further configured to generate a report if it is determined that one or more of the identified requests indicate the attack characterized by the predefined pattern, said report providing information regarding the characterized attack for use in defending against the attack.

22. The system of claim 16, wherein the processor is further configured to remedy the characterized attack if it is determined that one or more of the identified requests indicate the characterized attack.

23. The system of claim 16, wherein the plurality of the requests comprises one or more of the following types of requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein the stored data comprises one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated.

24. The system of claim 23, wherein said predefined pattern is characterized by one or more of the following: using multiple test strings to unsuccessfully attempt a quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to attempt unsuccessfully the quantity of the requests on multiple human interaction proof strings within the predefined time interval.

25. The system of claim 16, further comprising means for determining whether the identified request indicates the attack characterized by the predefined pattern.

26. A user authentication system comprising:

a first memory area to store data relating to a plurality of requests communicated from a plurality of user agents;

a second memory area to store a predefined pattern of one or more requests, said predefined pattern characterizing an attack; and

a processor configured to execute computer-executable instructions to:

search the stored data based on a query variable to generate a result set that identifies at least one of the plurality of the requests communicated from at least one of the plurality of the user agents, and

compare each of the identified requests with the predefined pattern to determine if the characterized attack has occurred.

27. The system of claim 26, wherein the stored data comprises one or more of the following: a network address from which one of the plurality of the requests is communicated; a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests; a failed password associated with the one of the plurality of the requests; a status of the one of the plurality of the requests; a time stamp indicating a date and time of the one of the plurality of the requests; a type of interface from which the one of the plurality of the requests is communicated; and a user agent from which the one of the plurality of the requests is communicated.

28. The system of claim 26, wherein said predefined pattern is characterized by one or more of the following: using a single password to unsuccessfully attempt at least

a predetermined quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the multiple user accounts within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the single network address within the predefined time interval.

29. The system of claim 26, wherein the processor is further configured to generate a report if the characterized attack is determined to have occurred, said report providing information regarding the characterized attack for use in defending against the attack.

30. The system of claim 26, wherein the processor is further configured to remedy the characterized attack if the characterized attack is determined to have occurred.

31. The system of claim 26, wherein the plurality of the requests comprises one or more of the following types of requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said predefined pattern is characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval, and using a single test string to unsuccessfully attempt at least

the predetermined quantity of the requests on multiple human interaction proof strings within the predefined time interval.

32. The system of claim 26, further comprising means for determining if the stored data associated with one or more of the plurality of the requests matches the predefined pattern.

33. One or more computer-readable media having computer-executable components for detecting an attack on an authentication service, said computer-readable media comprising:

a memory component to store data relating to a plurality of requests communicated to an authentication service from a plurality of user agents via a data communication network,

a query component to search the stored data as a function of a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user agents, and

an analyzing component to compare the stored data associated with each of the identified requests with a predefined pattern characterizing an attack to determine when the identified request indicates the characterized attack on the authentication service.

34. The computer-readable media of claim 33, wherein the stored data comprises one or more of the following information: a network address from which one of the plurality of the requests is communicated; a credential type of the one of the

plurality of the requests; a user account associated with the one of the plurality of the requests; a failed password associated with the one of the plurality of the requests; a status of the one of the plurality of the requests; a time stamp indicating a date and time of the one of the plurality of the requests; a type of interface from which the one of the plurality of the requests is communicated; and the user agent from which the one of the plurality of the requests is communicated.

35. The computer-readable media of claim 33, wherein said predefined pattern is characterized by one or more of the following: using a single password to unsuccessfully attempt a quantity of requests on multiple user accounts within a predefined time interval; using the single password to unsuccessfully attempt the quantity of the requests from a single network address on the multiple user accounts within the predefined time interval; and unsuccessfully attempting the quantity of the requests from the single network address within the predefined time interval.

36. The computer-readable media of claim 33, further comprising a report component to generate a report if it is determined that one or more of the identified requests indicate the characterized attack, said report providing information regarding the attack for use in defending against the attack.

37. The computer-readable media of claim 33, further comprising a defense component to remedy the characterized attack if it is determined that one or more of the identified requests indicate the characterized attack.

38. The computer-readable media of claim 37, wherein said defense component is adapted to remedy the characterized attack by performing one or more of the following: locking a user account associated with one of the plurality of the requests; blocking a network address from which the one of the plurality of the requests is communicated; implementing a human interaction proof on the authentication service; prompting a user to change a password associated with the user account; and limiting a quantity of allowed unsuccessful requests to a predetermined quantity within a predefined time interval for the network address from which the one of the plurality of the requests is communicated.

39. The computer-readable media of claim 33, wherein the plurality of the requests comprises one or more of the following types of requests: authentication, registration, and password-reset; wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said predefined pattern is characterized by one or more of the following: using multiple test strings to unsuccessfully attempt a quantity of requests on a single human interaction proof string within a predefined time interval, and using a single test string to unsuccessfully attempt the quantity of the requests on multiple human interaction proof strings within the predefined time interval.

40. The computer-readable media of claim 33, wherein the query component is adapted to search the stored data to identify at least one of the plurality of the requests

by generating a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts, and a time interval during which one or more requests are communicated; and wherein the result set identifies the stored data relating to one or more requests that match the query variables.